Practitioner's Docket No. NAI1P462/01.059.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Neil John Hursey et al.

Application No.: 09/912,391 Group No.: 2131
Filed: 07/26/2001 Examiner: Henning, Matthew T.
For: DETECTING E-MAIL PROPAGATED MALWARE

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 11/16/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 12/19/2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351(Order No.NAIIP462).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351(Order No.NAIIP462).

Date: January 19, 2007

/KEVINZILKA/

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Hursey et al.	)	Group Art Unit: 2131
	)	
Application No. 09/912,391	)	Examiner: Henning, Matthew T.
	)	
Filed: 07/26/2001	)	Date: 01/19/2007
	)	
For: DETECTING E-MAIL PROPAGATED MALWARE	)	
	)	
	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 11/16/2006, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 12/19/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-4, 6-12, 14-20, and 22-28

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-4, 6-12, 14-20, and 22-28
3. Claims allowed: None
4. Claims rejected: 1-4, 6-12, 14-20, and 22-28
5. Claims cancelled: 5, 13, and 21

C. CLAIMS ON APPEAL

The claims on appeal are: 1-4, 6-12, 14-20, and 22-28

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, an amendment was filed 10/12/2005 in response to a final Office Action mailed 5/26/2005, and such amendment was entered after the filing of an RCE.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1, 3, and 4, a computer program product operable to control an e-mail client computer to detect e-mail propagated malware is provided. The computer program product includes e-mail generating logic which is operable to generate an e-mail message (e.g. see item 4 of Figure 1, etc.), as well as comparison logic operable to compare the e-mail message with at least one of an address book of a sender of the e-mail message and one or more previously generated e-mail messages from the client computer (e.g. see item 12 of Figure 3, and item 32 of Figure 4 etc.). Additionally, identifying logic is included that is operable to identify whether (i) the e-mail message is being sent to more than a threshold number of addressees specified within the address book (e.g. see item 14 of Figure 3, etc.). Further, the identifying logic is also operable to identify whether (ii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of the previously generated e-mail messages being sent to more than a threshold number of addressees specified within the address book (e.g. see item 42 of Figure 4, etc.). In addition, the identifying logic is also operable to identify whether (iii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of the previously generated e-mail messages (e.g. see item 42 of Figure 4, etc.). The identifying logic is further operable to identify the email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified. Further, the computer program product comprises quarantine queue logic operable to hold the previously generated e-mail messages in a quarantine queue (e.g. see step 28 of Figure 3, etc.) for at least a predetermined quarantine period prior to being sent from the client computer. See, for example, page 2, line 30 – page 3, line 14; and page 4, lines 8-12 and lines 24-29 et al.

With respect to a summary of Claim 9, as shown in Figures 1, 3, and 4, a method of detecting e-mail propagated malware within an e-mail client computer is provided. In use, an e-mail message is generated (e.g. see item 10 of Figure 3, etc.) and the e-mail message is compared with at least one of an address book of a sender of the e-mail message and one or more previously generated e-mail messages from the client computer (e.g. see item 12 of Figure 3, and item 32 of Figure 4 etc.). Further, it is identified whether (i) the e-mail message is being sent to more than a

threshold number of addressees specified within the address book (e.g. see item 14 of Figure 3, etc.), (ii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of the previously generated e-mail messages being sent to more than a threshold number of addressees specified within the address book (e.g. see item 42 of Figure 4, etc.), and (iii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of the previously generated e-mail messages (e.g. see item 42 of Figure 4, etc.). In addition, the email message is identified as potentially containing malware if at least one of items (i), (ii), and (iii) is identified. Still yet, previously generated e-mail messages are held in a quarantine queue (e.g. see step 28 of Figure 3, etc.) for at least a predetermined quarantine period prior to being sent from the client computer. See, for example, page 2, line 30 – page 3, line 14; and page 4, lines 8-12 and lines 24-29 et al.

With respect to a summary of Claim 17, as shown in Figures 1, 3, and 4, an apparatus for detecting e-mail propagated malware within a client computer is provided. In use, an e-mail generator is operable to generate an e-mail message (e.g. see item 4 of Figure 1, etc.) and a comparator is operable to compare the e-mail message with at least one of an address book of a sender of the e-mail message and one or more previously generated e-mail messages from the client computer (e.g. see item 12 of Figure 3, and item 32 of Figure 4 etc.). Additionally, a malware identifier is operable to identify whether (i) said e-mail message is being sent to more than a threshold number of addressees specified within the address book (e.g. see item 14 of Figure 3, etc.), (ii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of the previously generated e-mail messages being sent to more than a threshold number of addressees specified within the address book (e.g. see item 42 of Figure 4, etc.), and (iii) the e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of the previously generated e-mail messages (e.g. see item 42 of Figure 4, etc.). In addition, the malware identifier is further operable to identify the email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified. Further, a quarantine queue is operable to hold the previously generated e-mail messages in a quarantine queue (e.g. see step 28 of Figure 3, etc.) for at least a predetermined quarantine period prior to being sent from the client

computer. See, for example, page 2, line 30 – page 3, line 14, and page 4, lines 8-12 and lines 24-29 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Issue # 2: The Examiner has rejected Claims 1-4, 6-12, 14-20, and 22-28 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue # 3: The Examiner has rejected Claims 1-3, 7, 9-11, 15, 17-19, 23, and 26 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462).

Issue # 4: The Examiner has rejected Claims 4, 6, 12, 14, 20, 22, and 27-28 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Bates et al. (U.S. Patent No. 6,785,732) (hereinafter Bates2).

Issue # 5: The Examiner has rejected Claims 8, 16, and 24 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Kouznetsov (U.S. Patent No. 6,725,377).

Issue # 6: The Examiner has rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Radatti (U.S. Patent No. 6,763,467).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

The Examiner has argued that "[t]he claim limitations regarding identifying whether (i), (ii), and (iii) in combination is not supported by the specification." Appellant respectfully disagrees and points out that page 6, lines 12-13 of the specification states that "the anti-virus mechanism 6 can apply the techniques described hereinafter to resist mass mailing malware," and also notes that page 9, lines 21-22 of the specification states that "the general purpose computer 200 operating under control of a suitable computer program may perform the above described techniques" (emphasis added). For these and other reasons, support for the combination of (i), (ii), and (iii) claimed in each of the independent claims is present. Of course, such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

Issue # 2:

The Examiner has rejected Claims 1-4, 6-12, 14-20, and 22-28 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Group #1: Claims 1-4, 6-12, 14-20, and 22-28

The Examiner has argued that "there is support for each of (i), (ii) and (iii) in the alternative, as shown in page 7 line 30 – page 8 line 15 of the present specification, but never as a combination." Appellant respectfully disagrees and points out that page 6, lines 12-13 of the specification states that "the anti-virus mechanism 6 can apply the techniques described hereinafter to resist mass mailing malware," and also notes that page 9, lines 21-22 of the

specification states that "the general purpose computer 200 operating under control of a suitable computer program may perform the above described techniques" (emphasis added). Thus, support for the combination of (i), (ii), and (iii) claimed in each of the independent claims is present. Of course, such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

Issue # 3:

The Examiner has rejected Claims 1-3, 7, 9-11, 15, 17-19, 23, and 26 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462).

Group #1: Claims 1-3, 7, 9-11, 15, 17-19, and 23

In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the third element of the *prima facie* case of obviousness, and particularly with respect to the independent claims, the Examiner has relied on Col. 9, lines 3-19 from the Bates reference to make a prior art showing of appellant's claimed "comparison logic operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer" (see this or similar, but not necessarily identical language in the independent claims).

> 'Block 94 illustrates comparing the new e-mail source address with the source addresses of e-mail received during a designated "B" time period. In particular, a rule designating the "B" time period is preferably included in spam filtering rules for the filter and may be

> adjusted by the prediction application executing on the server or by an alternate source. Next, block 98 depicts a determination as to whether or not the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients. If the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients, then the process passes to block 120. If the number of users receiving e-mail from the same source address during the "B" time period is not greater than a designated "C" number of recipients, then the process passes to block 100.' (Col. 9, lines 3-19)

Appellant respectfully notes that the excerpt from Bates relied on by the Examiner simply teaches 'comparing the new e-mail source address with the source addresses of e-mail received during a designated "B" time period' (emphasis added). Clearly, in Bates, a new e-mail source address is only compared with e-mail received, which does not meet "compare[ing] said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer" where "said previously generated e-mail messages [are held] in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer," in the context specifically claimed by appellant (emphasis added).

Additionally, with respect to the independent claims, the Examiner has relied on Col. 9, line 64 – Col. 10, line 10 from the Bates reference to make a prior art showing of appellant's claimed "identifying logic operable to identify whether said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" (see this or similar, but not necessarily identical language in the independent claims).

> "Block 112 illustrates comparing the content of e-mails that are the same size as the new e-mail with the content of the new e-mail. Spam filtering rules designated at the server preferably designate grouping of previously received e-mails that may be utilized for size comparison. Thereafter, block 114 depicts a determination as to whether or not substantial similarities in content are found between the new e-mail and a particular amount of same sized e-mail. If there are substantial similarities in content between the new e-mail and a particular amount of same sized e-mail, then the process passes to block 120. If there are not substantial similarities in content between the new e-mail and a particular amount of same sized e-mail, then the process passes to block 116." (Col. 9, line 64 – Col. 10, line 10)

Appellant respectfully asserts the excerpt from Bates relied on by the Examiner merely discloses "comparing the content of e-mails that are the same size as the new e-mail with the content of the new e-mail" (emphasis added). However, appellant claims a technique where "said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," in the context claimed (emphasis added). Appellant notes that simply nowhere in Bates is there any disclosure of "e-mail messages being sent to more than a threshold number of addressees specified within said address book," in the context claimed by appellant (emphasis added).

Additionally, appellant respectfully points out block 98 in Fig. 4A of the Bates reference, which 'depicts a determination as to whether or not the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients' (Col. 9, lines 9-12). In Fig. 4A, if the determination in block 98 results in an affirmative, or "YES," result, the process **skips block 114**, which "depicts a determination as to whether or not substantial similarities in content are found between the new e-mail and a particular amount of same sized e-mail" (Col. 10, lines 1-4), and instead proceeds directly to block 120, which "illustrates marking the new e-mail as predicted spam" (Col. 10, lines 17-18). Clearly, this fails to meet, and even *teaches away* from appellant's claimed "identifying logic operable to identify whether...said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," as claimed (emphasis added).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that it would have been obvious to combine Bates with Marsh because 'the ordinary person skilled in the art would have been motivated to provide means of detecting viral spam as suggested by Marsh, as well as giving the user the final say in what is to be done with detected viral spam...[and that] in this combination it would be obvious that the messages would be held in a "quarantine" for a predetermined amount of time prior to sending in order for the user to have the option of deleting

the messages detected as being viral spam without sending the messages.' To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Bates and Marsh references, especially in view of the vast evidence to the contrary.

For example, the Bates reference teaches that "[i]n accordance with the present invention, multiple e-mails are received at a network server intended for multiple clients served by the network server" (see Abstract) and that '[b]lock 92 depicts a determination as to whether or IC not the number of recipients of the new e-mail is greater that a designated "A" number of recipients...[where] a rule designating the "A" number of recipients is preferably included in spam filtering rules for the server' (see Bates Col. 8, lines 56-60). On the other hand, the Marsh reference teaches that "the virus detection utility 104 may be an add in program organized into a conventional format such as a plug-in for the e-mail application 102" where "[f]or example, the virus detection utility 104 [is] stored as a dynamic link library (DLL) file and...include[s] routines to execute in conjunction with the e-mail application 102 to perform specific operations" (see Marsh Col. 2, lines 26-33).

Clearly, in Marsh, the virus detection utility runs on clients in conjunction with email applications located on such clients, and utilizes client-based information (e.g. address books), whereas, in Bates, a server is used to receive emails sent to clients and to predict undesirable emails utilizing rules stored on the server. Thus, Marsh clearly *teaches away* from Bates. Appellant respectfully points out that it is improper to combine references where the references *teach away* from their combination. *In re Grasselli*, 713 F.2d 732, 743, 218 USPQ 769, 779 (Fed. Circ. 1983).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as also noted above.

Group #2: Claim 26

With respect to dependent Claim 26, the Examiner has relied on Col. 1, line 66 – Col. 2, line 7 in Bates to make a prior art showing of appellant's claimed technique "wherein said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment."

> "The sending and receiving of unsolicited e-mail messages are increasing problems for both ISPs and corporations. In particular, unsolicited sending and receiving of e-mail can unnecessarily utilize data storage space on servers and for ISPs unsolicited mail reduces customer satisfaction. In addition, unsolicited mail may includes viruses, worms, or other destructive attachments that can easily be transmitted within a server upon activation at a single client within a network." (Col. 1, line 66 – Col. 2, line 7)

Appellant respectfully asserts that such excerpt from Bates only discloses that "other destructive attachments…can easily be transmitted within a server upon activation of a single client within a network." Clearly, only mentioning an attachment, as in Bates, does not even suggest appellant's specific claim language, namely that "said e-mail message is identified as potentially containing malware **when** said e-mail message and said previously generated e-mail messages share a common attachment," as claimed (emphasis added).

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 4:

The Examiner has rejected Claims 4, 6, 12, 14, 20, 22, and 27-28 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Bates et al. (U.S. Patent No. 6,785,732) (Bates2).

Group #1: Claims 4, 6, 12, 14, 20, and 22

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #3, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 27

With respect to dependent Claim 27, the Examiner has relied on Col. 8, paragraph 1 in Bates2 to make a prior art showing of appellant's claimed technique "wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware."

> "..Method 400 begins when a web client requests information that normally would flow through the web server to the web client (step 410). If the request does not require virus checking (step 420=NO), the requested information is sent to the web client (step 480). If the request requires virus checking (step 420=YES), a virus check is performed on the requested information (step 430). If no virus is found (step 440=NO), the requested information is sent to the web client (step 480). If a virus is found (step 440=YES), the web client is notified of the virus (step 450), and an entry is made in the virus information database (step 460) regarding the name of the virus, type, when detected, etc. Finally, the appropriate authorities may be notified of the virus (step 470). The term "appropriate authorities" is a broad term that encompasses anyone who may need to know about the occurrence of a virus, including a network administrator of a local area network, a web site administrator, a contact person in a virus detection company, and appropriate law enforcement officials, such as local, state, federal, and international law enforcement agencies." (Col. 8, paragraph 1 - emphasis added)

Appellant respectfully asserts that the excerpt from Bates2 relied upon by the Examiner merely discloses that "[i]f a virus is found... the web client is notified of the virus (step 450)" and that "the appropriate authorities may be notified of the virus" (emphasis added). However, the mere disclosure that if a virus is found, the appropriate authorities may be notified of the virus, as in Bates2, simply fails to even suggest a technique "wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware," as claimed by appellant (emphasis added). Clearly, the mere disclosure of notifying the appropriate authorities of the found virus,

as in Bates2, simply fails to suggest "provid[ing] a warning of new malware outbreaks," in the manner as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 28

With respect to dependent Claim 28, the Examiner has relied on Col. 8, paragraph 1 in Bates2 (reproduced above) to make a prior art showing of appellant's claimed technique "wherein said message to said malware computer program provider includes a copy of said e-mail message."

Appellant respectfully asserts that the excerpt from Bates2 relied upon by the Examiner merely discloses that "[i]f a virus is found... the web client is notified of the virus (step 450)" and that "the appropriate authorities may be notified of the virus" (emphasis added). However, the general disclosure that if a virus is found, the appropriate authorities may be notified of the virus, as in Bates2, simply fails to even suggest a specific technique "wherein said message to said malware computer program provider includes a copy of said e-mail message," as claimed by appellant (emphasis added). Clearly, the mere disclosure of notifying the appropriate authorities of the found virus, as in Bates2, simply fails to suggest that the "message to said malware computer program provider includes a copy of said e-mail message," in the manner as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 5:

The Examiner has rejected Claims 8, 16, and 24 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Kouznetsov (U.S. Patent No. 6,725,377).

Group #1: Claims 8, 16, and 24

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #3, Group #1.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 6:

The Examiner has rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Radatti (U.S. Patent No. 6,763,467).

Group #1: Claim 25

With respect to dependent Claim 25, the Examiner has relied on Col. 1, lines 36-48 of the Radatti reference to make a prior art showing of appellant's claimed technique "wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing."

> "Virus, worms, and trojan horses can infect an internal network or single computer system when the internal network or computer system executes a program from the external network that contains the hostile algorithm. All binary executables, unreviewed shell scripts, and source code accessed from an external network may contain worms, viruses, or trojan horses. In addition, outside binary executables, shell scripts, and scanned source code may enter an internal network or single computer system through an E-mail attachment. Also, executables can be directly accessed from an external network through the IFTP program, a world-wide web browser, or an outside contractor whose network already has been compromised." (Col. 1, lines 36-48)

Specifically, appellant notes that the Examiner has argued that "Radatti teaches that only executable code may contain malware." Appellant respectfully disagrees and points out that the excerpt from Radatti merely discloses that "[a]ll binary executables, unreviewed shell scripts, and source code accessed from an external network may contain worms, viruses, or trojan horses" and that "outside binary executables, shell scripts, and scanned source code may enter an internal network or single computer system through an E-mail attachment" (emphasis added). Clearly, disclosing that binary executables may contain worm, viruses, or Trojan horses, as in Radatti, does not suggest that "only executable code may contain malware," as noted by the Examiner (emphasis added). Furthermore, simply disclosing that executables may contain worms, viruses, or Trojan horses, as in Radatti, does not specifically teach any sort of e-mail, let alone meet appellant's specifically claimed technique "wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, **to speed processing**," as claimed by appellant (emphasis added).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product operable to control an e-mail client computer to detect e-mail propagated malware, said computer program product comprising:

e-mail generating logic operable to generate an e-mail message;

comparison logic operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer; and

identifying logic operable to identify whether:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said identifying logic is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

quarantine queue logic operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

2. (Original) A computer program product as claimed in claim 1, wherein said e-mail message specifies a plurality of addressees, said comparison logic being operable to compare said plurality of addressees with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

3. (Original) A computer program product as claimed in claim 1, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

4. (Original) A computer program product as claimed in claim 3, wherein said proportion of addressees within said address book is user specified.

5. (Cancelled)

6. (Previously Presented) A computer program product as claimed in claim 1, wherein said quarantine period is user specified.

7. (Original) A computer program product as claimed in claim 1, comprising confirmation input logic operable when said e-mail message is identified as potentially containing malware to generate a user message seeking a confirmation input from a user of said client computer before said e-mail message is sent.

8. (Original) A computer program product as claimed in claim 1, comprising administrator warning logic operable when said e-mail message is identified as potentially containing malware to send an administrator warning message to an administrator of said client computer regarding said e-mail message.

9. (Previously Presented) A method of detecting e-mail propagated malware within an e-mail client computer, said method comprising the steps of:

generating an e-mail message;

comparing said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

identifying whether:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said email message is identified as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

holding said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

10. (Original) A method as claimed in claim 9, wherein said e-mail message specifies a plurality of addressees, said plurality of addressees being compared with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

11. (Original) A method as claimed in claim 9, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

12. (Original) A method as claimed in claim 11, wherein said proportion of addressees within said address book is user specified.

13. (Cancelled)

14. (Previously Presented) A method as claimed in claim 9, wherein said quarantine period is user specified.

15. (Original) A method as claimed in claim 9, wherein when said e-mail message is identified as potentially containing malware, then a user message is generated seeking a confirmation input from a user of said client computer before said e-mail message is sent.

16. (Original) A method as claimed in claim 9, wherein when said e-mail message is identified as potentially containing malware, then an administrator warning message is sent to an administrator of said client computer regarding said e-mail message.

17. (Previously Presented) Apparatus for detecting e-mail propagated malware within a client computer, said apparatus comprising:

an e-mail generator operable to generate an e-mail message;

a comparitor operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

a malware identifier operable to identify whether:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said malware identifier is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

a quarantine queue operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer.

18. (Original) Apparatus as claimed in claim 17, wherein said e-mail message specifies a plurality of addressees, said comparitor being operable to compare said plurality of addressees with said e-mail address book to determine if said at least a threshold number of addressees has been exceeded.

19. (Previously Presented) Apparatus as claimed in claim 17, wherein said at least a threshold number of addressees is specified as a proportion of addressees within said address book.

20. (Original) Apparatus as claimed in claim 19, wherein said proportion of addressees within said address book is user specified.

21. (Cancelled)

22. (Previously Presented) Apparatus as claimed in claim 17, wherein said quarantine period is user specified.

23. (Original) Apparatus as claimed in claim 17, comprising a confirmation input unit operable when said e-mail message is identified as potentially containing malware to generate a user message seeking a confirmation input from a user of said client computer before said e-mail message is sent.

24. (Original) Apparatus as claimed in claim 17, comprising an administrator warning unit operable when said e-mail message is identified as potentially containing malware to send an administrator warning message to an administrator of said client computer regarding said e-mail message.

25. (Previously Presented) A computer program product as claimed in claim 1, wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing.

26. (Previously Presented) A computer program product as claimed in claim 1, wherein said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment.

27. (Previously Presented) A computer program product as claimed in claim 1, wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware.

28. (Previously Presented) A computer program product as claimed in claim 27, wherein said message to said malware computer program provider includes a copy of said e-mail message.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P462/01.059.01).

Respectfully submitted,

By: /KEVINZILKA/ Date: January 19, 2007

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660